

# Table des matières

<b>1. Les congruences.....</b>	<b>1</b>
1.1. Introduction .....	1
1.2. La notion de congruence.....	1
1.3. Quelques propriétés des congruences.....	3
1.4. Opérations sur les congruences .....	4
1.5. Les puissances en arithmétique modulaire .....	7
1.6. Congruence inverse .....	8
1.7. Les diviseurs de zéro .....	14
1.8. Rappel : le petit théorème de Fermat.....	15
1.9. Identités remarquables.....	17
1.10. L'arithmétique modulaire modulo 9.....	17
1.11. Le cas des additions et multiplications modulo 2.....	19
1.12. Exercices.....	19
1.13. Démonstration du théorème de Wilson .....	21
1.14. L'exponentiation modulaire rapide .....	22
1.15. Théorème de Wolstenholme.....	23
1.16. Équation aux congruences. Congruence avec exposant .....	25
1.17. Exercices.....	26
1.18. Nombres parfaits .....	30
1.19. Entiers de Gauss et congruences ?.....	30
<b>2. Congruence d'une puissance.....</b>	<b>33</b>
2.1. Les carrés dans l'ensemble $\mathbb{Z}/n\mathbb{Z}$ .....	33
2.2. Les cubes modulo $n$ .....	35
2.3. Propriétés de base .....	37
2.4. Congruences et puissances modulo $p^n$ .....	40
2.5. Somme des puissances dans $\mathbb{Z}/n\mathbb{Z}$ .....	42
2.6. Les inverses modulo $p^2$ .....	43
2.7. Les inverses modulo $p^n$ .....	44
2.8. Carré inversible modulo $p$ .....	44
2.9. Les racines carrées modulo $n$ .....	46
2.10. Congruence quadratique (ou de Legendre).....	48
2.11. Exercices.....	49
2.12. Conclusion.....	54
<b>3. Les polynômes en arithmétique modulaire.....</b>	<b>55</b>
3.1. Introduction .....	55
3.2. Les opérations de base.....	56
3.3. La division euclidienne.....	56
3.4. Le PGCD de deux polynômes .....	57

3.5.	Polynômes premiers entre eux.....	57
3.6.	Théorème de Gauss .....	58
3.7.	Polynômes irréductibles .....	58
3.8.	Racines de congruence .....	58
3.9.	Polynômes congrus.....	59
3.10.	La factorisation des polynômes .....	60
3.11.	Pour approfondir.....	62
3.12.	Conclusion.....	62
<b>4.</b>	<b>Les résidus quadratiques.....</b>	<b>63</b>
4.1.	Introduction .....	63
4.2.	Les résidus quadratiques.....	64
4.3.	Déterminer si un nombre est résidu quadratique .....	66
4.4.	Exercice .....	69
4.5.	Propriétés élémentaires des résidus quadratiques.....	70
4.6.	Quelques lemmes démontrés par Gauss .....	70
4.7.	Sommes et produits de résidus quadratiques .....	74
4.8.	Résidus associés .....	76
4.9.	Application à la résolution d'équations diophantiennes.....	77
4.10.	Exercice .....	77
4.11.	Résidus quadratiques modulo $p^2$ ou $p^n$ .....	77
4.12.	Les nombres de Blum.....	78
4.13.	Application aux équations diophantiennes du second degré .....	79
4.14.	Exercices.....	80
4.15.	Conclusion.....	84
4.16.	Pour approfondir.....	85
<b>5.</b>	<b>Le symbole de Legendre .....</b>	<b>87</b>
5.1.	Définition.....	87
5.2.	La loi de réciprocité quadratique .....	88
5.3.	Propriétés du symbole de Legendre.....	89
5.4.	Lemme de Gauss .....	90
5.5.	Quelques cas particuliers .....	91
5.6.	Méthodes de calcul du symbole de Legendre.....	95
5.7.	Démonstration des lemmes du chapitre précédent .....	96
5.8.	Valeurs du symbole de Legendre .....	97
5.9.	Exercices.....	98
5.10.	Conclusion.....	102
<b>6.</b>	<b>Le symbole de Jacobi .....</b>	<b>103</b>
6.1.	Définition.....	103
6.2.	Quelques propriétés de base .....	104
6.3.	Symbole de Jacobi et loi de réciprocité quadratique .....	105
6.4.	Lien avec la factorisation.....	107
6.5.	Exercices.....	107
6.6.	Conclusion.....	109

<b>7. Les résidus cubiques et biquadratiques .....</b>	<b>111</b>
7.1. Introduction .....	111
7.2. Définitions .....	111
7.3. Propriété commune aux résidus cubiques et biquadratiques .....	111
7.4. Les résidus cubiques.....	112
7.5. Les résidus biquadratiques.....	119
7.6. Conclusion.....	123
7.7. Pour approfondir.....	123
7.8. Récapitulation des résidus quadratiques, cubiques et biquadratiques ..	123
<b>8. Ordre d'un élément.....</b>	<b>125</b>
8.1. Ordre d'un élément.....	125
8.2. Propriétés élémentaires de l'ordre .....	127
8.3. Quelques lemmes.....	128
8.4. A propos de l'indicatrice d'Euler .....	130
8.5. La fonction $\Psi$ .....	130
8.6. L'indicatrice de Carmichaël .....	132
8.7. Exercices.....	134
8.8. Conclusion.....	135
<b>9. Racine primitive .....</b>	<b>137</b>
9.1. Rappels : groupes et sous-groupes cycliques.....	137
9.2. Puissances en arithmétique modulaire.....	138
9.3. Définition.....	138
9.4. Combien de racines primitives dans un groupe.....	140
9.5. Théorème de la racine primitive .....	141
9.6. Recherche des racines primitives .....	142
9.7. Propriétés élémentaires des racines primitives .....	144
9.8. Produit de racines primitives .....	145
9.9. Racines primitives et résidus quadratiques ou cubiques.....	146
9.10. Exercice .....	148
9.11. Racines primitives modulo un nombre composé.....	149
9.12. Monsieur Tompkins et les racines primitives.....	150
9.13. Pour approfondir.....	151
<b>10. Le logarithme discret .....</b>	<b>153</b>
10.1. Rappels : la fonction logarithme.....	153
10.2. Définition.....	153
10.3. Quelques propriétés élémentaires .....	155
10.4. Cas d'un groupe non cyclique .....	157
10.5. Recherche du logarithme discret .....	158
10.6. L'échange de clés de Diffie-Hellman .....	160
10.7. Conclusion.....	161
<b>11. Les équations du 1<sup>er</sup> degré.....</b>	<b>163</b>
11.1. Généralités.....	163
11.2. Équations linéaires aux congruences.....	163

---

11.3.	Système d'équations linéaires portant sur les congruences .....	165
11.4.	Exercices.....	167
<b>12.</b>	<b>Les équations de degré 2.....</b>	<b>173</b>
12.1.	Les équations de degré 2 modulo un nombre premier.....	173
12.2.	Le cas général.....	175
12.3.	Exercices.....	177
12.4.	Conclusion.....	179
<b>13.</b>	<b>Les équations de degré supérieur à 2 .....</b>	<b>181</b>
13.1.	Les équations modulo un nombre premier .....	181
13.2.	Le lemme du relèvement .....	182
13.3.	Équation diophantienne $x^2 + 3y^2 = z^3$ .....	183
13.4.	L'équation $ax^4 = b \pmod n$ .....	184
13.5.	Conjecture de Catalan et dérivées .....	184
13.6.	Équation avec l'inconnue en exposant .....	184
13.7.	Congruence de carrés.....	185
13.8.	Exercices.....	185
13.9.	Pour approfondir.....	187
<b>14.</b>	<b>Les grands nombres premiers ou pseudo-premiers.....</b>	<b>189</b>
14.1.	Introduction .....	189
14.2.	Définitions.....	189
14.3.	Le test de Fermat .....	191
14.4.	Un théorème d'Euler .....	192
14.5.	Le cas des nombres premiers de Mersenne et de Proth .....	193
14.6.	Utilisation du théorème de la racine primitive .....	198
14.7.	Le test de primalité de Solovay-Strassen.....	200
14.8.	Le test de non-primalité de Rabin Miller.....	201
14.9.	Autres tests .....	204
14.10.	Conclusion.....	204
<b>15.</b>	<b>La factorisation de grands nombres.....</b>	<b>205</b>
15.1.	La factorisation classique .....	205
15.2.	Algorithme $p - 1$ de John Pollard.....	207
15.3.	Algorithme Rho de John Pollard .....	209
15.4.	Autres méthodes de factorisation .....	211
15.5.	Exercice .....	211
15.6.	Pour approfondir.....	211
<b>16.</b>	<b>La construction de grands nombres premiers.....</b>	<b>213</b>
16.1.	Nombres robustes .....	213
16.2.	La fabrication de nombres premiers robustes.....	214
16.3.	Mise en œuvre .....	217
16.4.	Conclusion.....	218
<b>17.</b>	<b>Ouverture vers la cryptographie .....</b>	<b>219</b>
17.1.	Introduction .....	219

---

17.2.	Les différentes approches de la cryptographie .....	220
17.3.	Les différentes techniques de chiffrement .....	221
17.4.	Le principe du système RSA .....	222
17.5.	Le système El Gamal .....	223
17.6.	L'authentification .....	224
17.7.	Quelques éléments de comparaison .....	225
17.8.	Pour approfondir .....	225
<b>18.</b>	<b>Les processeurs d'arithmétique modulaire .....</b>	<b>227</b>
18.1.	Introduction .....	227
18.2.	Les processeurs de ST Microelectronics .....	227
18.3.	L'unité de calcul modulaire de SUN .....	228
18.4.	Les processeurs d'IBM .....	228
18.5.	Les opérations .....	228
18.6.	Langages de programmation .....	228
18.7.	Conclusion .....	229
<b>19.</b>	<b>Annexe A : Les nombres de Mersenne .....</b>	<b>231</b>
19.1.	Définition des nombres de Mersenne .....	231
19.2.	Théorèmes portant sur les nombres de Mersenne .....	232
19.3.	Les nombres de Mersenne généralisés .....	232
19.4.	Conjectures .....	233
<b>20.</b>	<b>Annexe B : Les nombres de Fermat .....</b>	<b>235</b>
20.1.	Définition .....	235
20.2.	Relation de récurrence entre nombres de Fermat .....	235
<b>21.</b>	<b>Annexe C : Les nombres de Carmichael .....</b>	<b>237</b>
21.1.	Définition .....	237
21.2.	Théorème de Korselt .....	237
21.3.	Construction de nombres de Carmichael .....	238
21.4.	Une infinité de nombres de Carmichael ? .....	239
<b>22.</b>	<b>Bibliographie .....</b>	<b>241</b>
	<b>Index alphabétique .....</b>	<b>243</b>